МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Казанский национальный исследовательский технический университет

им. А.Н. Туполева – КАИ»

Институт компьютерных технологий и защиты информации

Отделение СПО ИКТЗИ (Колледж информационных технологий)

ЛАБОРАТОРНАЯ РАБОТА №3

по дисциплине

Информационная безопасность

Тема: «Обоснование применения норм уголовного права в конкретных ситуациях и нахождение применимых правовых норм в заданных условиях»

Работу выполнил

Студент гр.4233

Валеев Д.Э.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

Часть 1

Цель работы

Обосновать применение норм правового наказания при использовании ВПО.

Результат выполнения работы

1. Проанализируйте приведенные ниже ситуации.

Ссылаясь на статьи «Уголовного кодекса Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 02.08.2019), какую ответственность несут люди в данных ситуациях.

1. Вы пишите на заказ на программы, которые заражает компьютер и подгружают вредоносные программы. При этом сами данным программным обеспечение не пользуетесь.

Данное действие нарушает статью 273.1 – “[Создание](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [распространение](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) или [использование](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) компьютерных [программ](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100036) либо [иной](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100023) [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_469788/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), заведомо предназначенных для несанкционированного уничтожение, [блокирования](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [модификации](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации или [нейтрализации](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100016) средств защиты компьютерной информации” и они наказываются ограничением свободы на срок до четырех лет, либо принудтельными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Системный администратор некоторой известной компании без ведома устанавливал по сети всем программу для удаленного администрирования RAdmin.

Установка без согласия пользователей может рассматриваться как распространение вредоносного ПО (ст. 273.1 УК РФ) и нести за собой наказание ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Также человек может понести ответственность за Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

3. Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей

В любом случае человек распространил ВПО в открытый доступ, поэтому ему грозит ст 273.1 УК РФ

4. Вы не распространяли вирус, но выложили его на GitHub.

В любом случае это является распространением ВПО и наказывается по 273 УК РФ.

5. Вам 17 лет, ради интереса распространили вредоносное программное обеспечение.

Человек несёт уголовную ответственность с 16 лет, ему также грозит статья 273.1 УК РФ, а также 272 УК РФ.

6. Вы разработали код вредоносной программы, но еще не воспользовались им.

Если каким либо образом узнать, что данное ВПО было заведомо предназначено для несанкционированного [уничтожения](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [блокирования](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [модификации](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации или [нейтрализации](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100016) средств защиты компьютерной информации, то грозит статья 273.1 УК РФ. Вредоносный код также может быть разработан в целях тестирования и защиты от него.

7. Вы гражданин РФ и используете вредоносное программное обеспечение исключительно за пределами Российской Федерации

Данное действие может включать в себя уголовное преследование как в России, так и в стране, пострадавшей от кибератаки. Также возможно экстрадиция в другую страну для судебного разбирательства. Если же действия будут совпадать с интересами РФ, то есть вероятность отбора в государственную “армию” хакеров.

Ответы на контрольные вопросы

1. Перечислите виды ответственности за использование не лицензионного программного обеспечения?

Использование нелицензионного программного обеспечения является нарушением авторских и смежных прав и влечет за собой административную (ст. 7.12. КоАП РФ), уголовную (ст. 146 УК РФ) и гражданско-правовую от-ветственность.

2. Как правильно лицензировать программное обеспечение?

Авторские права: Перед лицензированием программы необходимо удостовериться, что у вас есть полные права на программное обеспечение или вы имеете право его распространять от имени правообладателя.

Выбор лицензионной модели: Существует множество лицензионных моделей, таких как открытая лицензия (например, GPL), проприетарная лицензия, условия лицензий на коммерческое использование и т. д. Выбор модели зависит от целей вашего бизнеса и условий, которые вы хотите установить для пользователей.

Соблюдение законодательства: Убедитесь, что ваша лицензия соответствует требованиям российского законодательства о защите авторских прав и программного обеспечения.

Права и обязанности сторон: В лицензионном соглашении следует четко определить права и обязанности как лицензиата, так и лицензиара, включая условия использования, ограничения, ответственность и т. д.

Регистрация и официальные документы: Хотя регистрация лицензионных соглашений в России не обязательна, но иногда это может быть полезным для обеспечения защиты ваших прав.

Вывод

Обосновал применение норм правового наказания при использовании ВПО.

Часть 2

Цели

Ознакомиться с правовой сферой в области информационной безопасности.

Результат выполнения лабораторной работы

2. Эти документы вместе составляют правовую основу для обеспечения информационной безопасности в Российской Федерации, они определяют правила и принципы защиты информации, персональных данных и государственных секретов.

3.

1. Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности»:

Содержит общие положения о национальной безопасности и меры по ее обеспечению, что включает в себя и информационную безопасность.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

Устанавливает основные принципы обращения с информацией, информационными технологиями и обеспечения их защиты, что является основой для обеспечения информационной безопасности.

3. Закон РФ «О государственной тайне» от 21.07.1993:

Регулирует порядок обращения с государственной тайной, что является важным аспектом обеспечения информационной безопасности государства.

4. Федеральный закон «О коммерческой тайне» от 29.07.2004:

Определяет понятие коммерческой тайны и устанавливает меры по ее защите, что также важно для обеспечения конфиденциальности информации и, следовательно, информационной безопасности.

5. Федеральный закон «О персональных данных» от 27.07.2006:

Устанавливает правила сбора, обработки и защиты персональных данных, что важно для обеспечения конфиденциальности информации и защиты прав граждан на приватность.

6. Федеральный закон «Об электронной подписи» от 06.04.2011:

Регулирует использование электронной подписи, что является важным средством обеспечения целостности и аутентичности информации в цифровой среде, что также связано с информационной безопасностью.

7. Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015):

Устанавливает меры по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена.

Ответы на контрольные вопросы

1. Для чего нужны законодательные меры в области информационной безопасности?

Законодательные меры в области информационной безопасности необходимы для защиты информации от угроз, связанных с ее несанкционированным доступом, утечкой, порчей и другими видами кибератак. Они также помогают регулировать использование информационных технологий и обеспечивать безопасность как в государственных, так и в частных секторах.

2. Какими документами регулируется информационная безопасность в Российской Федерации?

* Федеральный закон "Об информации, информационных технологиях и о защите информации"
* Федеральный закон "О защите информации в информационно-телекоммуникационных сетях"
* Постановление Правительства РФ "Об утверждении Правил учета, хранения, использования и распространения сведений, составляющих государственную тайну, содержащихся в средствах вычислительной техники"

3. Какие основополагающие документы в области информационной безопасности вам известны?

ISO/IEC 27001: Этот стандарт определяет требования к системам управления информационной безопасностью (СУИБ), помогая организациям управлять и защищать свою информацию и активы.

ISO/IEC 27002: Также известный как "Информационная технология. Методы и средства обеспечения безопасности. Практическое руководство по управлению информационной безопасностью". Этот документ содержит рекомендации и практические руководства по обеспечению безопасности информации в организациях.

NIST SP 800 Series: Серия публикаций Национального института стандартов и технологий (NIST) США по информационной безопасности. В этой серии рассматриваются различные аспекты информационной безопасности, включая руководства, методики и стандарты.

GDPR (General Data Protection Regulation): Это регуляторный документ Европейского союза, который регулирует защиту данных и конфиденциальность граждан ЕС.

HIPAA (Health Insurance Portability and Accountability Act): Законодательный акт США, регулирующий защиту медицинской информации и конфиденциальность пациентов.

PCI DSS (Payment Card Industry Data Security Standard): Этот стандарт устанавливает требования по обработке, хранению, передаче и защите информации о платежных картах.

Cybersecurity Framework (CSF) от NIST: Этот документ предоставляет руководство по улучшению кибербезопасности организации путем применения согласованных фреймворков, стандартов и практик.

Вывод

Ознакомился с правовой сферой в области информационной безопасности.